Release Notes for Cisco Catalyst 9500 Series Switches, Cisco IOS XE Fuji 16.9.x

Introduction

Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance are Cisco's lead, fixed core and aggregation enterprise switching platforms. They have been purpose-built to address emerging trends of Security, IoT, Mobility, and Cloud.

They deliver complete convergence in terms of ASIC architecture with Unified Access Data Plane (UADP) 2.0 on Cisco Catalyst 9500 Series Switches and UADP 3.0 on Cisco Catalyst 9500 Series Switches - High Performance. The platform runs an Open Cisco IOS XE that supports model driven programmability, has the capacity to host containers, and run 3rd party applications and scripts natively within the switch (by virtue of x86 CPU architecture, local storage, and a higher memory footprint). The series forms the foundational building block for SD-Access, which is Cisco’s lead enterprise architecture.

Note
With the introduction of the High Performance models in the series, there may be differences in the supported and unsupported features, limitations, and caveats that apply to the Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance models. Throughout this release note document, any such differences are expressly called out. If they are not, the information applies to all models in the series.

Note
Explore the Content Hub, the all new portal that offers an enhanced product documentation experience.

- Use faceted search to locate content that is most relevant to you.
- Create customized PDFs for ready reference.
- Benefit from context-based recommendations.

Get started with the Content Hub at content.cisco.com to craft a personalized documentation experience.
Do provide feedback about your experience with the Content Hub.
Whats New in Cisco IOS XE Fuji 16.9.2

Software Features in Cisco IOS XE Fuji 16.9.2

Software Features Introduced on Cisco Catalyst 9500 Series Switches
(C9500-12Q, C9500-16X, C9500-24Q, C9500-40X)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description, License Level Information, Documentation Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>In Service Software Upgrade (ISSU)</td>
<td>A process that allows Cisco IOS software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco IOS software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades.</td>
</tr>
</tbody>
</table>

Note: Starting with this release, this feature is supported on the following models of the Cisco Catalyst 9500 Series Switches, with the Cisco Stackwise Virtual feature:

• C9500-24Q
• C9500-12Q
• C9500-40X
• C9500-16X

(Network Advantage)

Whats New in Cisco IOS XE Fuji 16.9.1

Hardware Features in Cisco IOS XE Fuji 16.9.1

• Hardware Features Introduced on Cisco Catalyst 9500 Series Switches
• Hardware Features Introduced on Cisco Catalyst 9500 Series Switches-High Performance
### Hardware Features Introduced on Cisco Catalyst 9500 Series Switches

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cisco 40GBASE QSFP Module (4x10G mode qualification) | • Supported transceiver module number—QSFP-40G-CSR4  
• Compatible switch models—C9500-12Q and C9500-24Q  
• Compatible network modules—C9500-NM-2Q uplinks  
For information about the module, see Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Cisco 40-Gigabit Ethernet Transceiver Modules Compatibility Matrix. |
For information about the module, see Cisco 40GBASE QSFP Modules Data Sheet. For information about device compatibility, see the Cisco 40-Gigabit Ethernet Transceiver Modules Compatibility Matrix. |
| USB 3.0 Solid State Drive (SSD) | A hot-pluggable drive that provides an extra 120GB storage for Kernel Virtual Machines (KVM) application hosting and Linux container (LXC) hosting. The storage drive can also be used to save packet captures, trace logs generated by the operating system, GIR snapshots and third-party applications.  
The module connects to the USB 3.0 port on the rear panel of the device.  
See Cisco Catalyst 9500 Series Switches Hardware Installation Guide → Installing Field Replaceable Units |
| A higher number of switch ports supported for QSFP-4X10G-LR-S | The QSFP-4X10G-LR-S module can now be installed on port numbers 1 through 12 of the C9500-12Q and C9500-24Q switch models. (Only port numbers 1 through 4 were supported in an earlier release). |
Hardware Features Introduced on Cisco Catalyst 9500 Series Switches—High Performance

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| Cisco 1000BASE-T SFP Transceiver Module | • Supported transceiver module product numbers—GLC-T, GLC-TE  
• Compatible switch models—C9500-48Y4C and C9500-24Y4C  
For information about the modules, see Cisco SFP Modules for Gigabit Ethernet Applications Data Sheet. For information about device compatibility, see the Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix. |
| Cisco 25GBASE SFP28 Transceiver Module—Cisco SFP-10/25G-CSR-S | • Supported transceiver module product numbers—Cisco SFP-10/25G-CSR-S  
• Compatible switch models—C9500-48Y4C and C9500-24Y4C  
For information about the module, see the Cisco 25GBASE SFP28 Modules Data Sheet. For information about compatibility with a device, see the Cisco 25-Gigabit Ethernet Transceiver Modules Compatibility Matrix. |
| Cisco QSFP 40-Gigabit Ethernet to SFP+ 10G Adapter Module (Cisco QSA Module)—CVR-QSFP-SFP10G | • Supported transceiver module product number—CVR-QSFP-SFP10G  
This module offers 10 Gigabit Ethernet and 1 Gigabit Ethernet connectivity for Quad Small Form-Factor Pluggable (QSFP)-only platforms by converting a QSFP port into an SFP or SFP+ port.  
• Compatible switch models—C9500-48Y4C and C9500-24Y4C uplink ports  
**Note** The module can now be installed on uplink ports. This was not supported when support for the module was first introduced in an earlier release.  
For information about the adapter, see the Cisco QSFP to SFP or SFP+ Adapter Module Data Sheet. For information about device compatibility, see the Cisco 40-Gigabit Ethernet Transceiver Modules Compatibility Matrix. |
| M.2 Serial Advanced Technology Attachment (SATA) Storage | Provides extra storage to host applications and to capture packet trace logs. M.2 SATA also supports Self-Monitoring, Analysis and Reporting Technology System (S.M.A.R.T.) attributes. You can monitor the health of SATA device through the S.M.A.R.T tools integrated in the Cisco IOS XE Fuji 16.9.1 image. |
Software Features in Cisco IOS XE Fuji 16.9.1

• Software Features Introduced on All Models
• Software Features Introduced on Cisco Catalyst 9500 Series Switches
• Software Features Introduced on Cisco Catalyst 9500 Series Switches-High Performance

Software Features Introduced on All Models

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description, License Level Information, Documentation Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graceful Insertion and Removal (GIR) enhancements</td>
<td>GIR is introduced on the High Performance models in this release. The feature uses a maintenance mode to isolate the switch from the network in order to perform debugging, or an upgrade. When you place the switch in maintenance mode, supported protocols are isolated, and Layer 2 interfaces are shut down. When normal mode is restored, the supported protocols and ports are brought back up. These enhancements have been added to the GIR feature in this release and are available on all models of the series:</td>
</tr>
<tr>
<td></td>
<td>• Snapshot templates can now be used to generate specific snapshots.</td>
</tr>
<tr>
<td></td>
<td>• Protocols belonging to one class within the same custom template are serviced in parallel.</td>
</tr>
<tr>
<td></td>
<td>• System mode maintenance counters have been added to track several events such as the number of times the switch went into maintenance.</td>
</tr>
<tr>
<td></td>
<td>See High Availability → Configuring Graceful Insertion and Removal.</td>
</tr>
<tr>
<td></td>
<td>(Network Advantage)</td>
</tr>
<tr>
<td>GIR Layer 2 protocol support for GIR Hot Standby Router Protocol (HSRP)</td>
<td>GIR is now supported for the HSRP protocol.</td>
</tr>
<tr>
<td></td>
<td>See High Availability → Configuring Graceful Insertion and Removal.</td>
</tr>
<tr>
<td></td>
<td>(Network Advantage)</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Description, License Level Information, Documentation Link</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| GIR Layer 2 protocol support for GIR Virtual Router Redundancy Protocol (VRRP) | GIR is now supported for the VRRP protocol.  
See High Availability → Configuring Graceful Insertion and Removal .  
(Network Advantage) |
| Hot Patching Support | Allows Software Maintenance Upgrade (SMU) to happen immediately after activation, without reloading the system.  
SMU is a package that can be installed on a system to provide a fix or a security resolution to a released image. The package is provided on a per release and per component basis.  
See System Management → Software Maintenance Upgrade .  
(Network Advantage for CLI and DNA Advantage for DNAC) |
| Media Access Control Security (MACsec): 256-bit AES MACsec (IEEE 802.1AE) host link encryption with MACsec Key Agreement (MKA) | Support for 256-bit AES MACsec (IEEE 802.1AE) encryption with MACsec Key Agreement (MKA) on the downlink ports is enabled.  
256-bit—(Network Advantage) |
| Media Access Control Security (MACsec) port channel support | Provides support for MACsec over port channels for Layer 2 and Layer 3 EtherChannels.  
128-bit—(Network Essentials and Network Advantage)  
256-bit—(Network Advantage) |
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description, License Level Information, Documentation Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>MACsec: XPN for 40 and 100 Gigabit Ethernet MACsec interfaces</td>
<td>The Extended Packet Numbering (XPN) feature in MKA or MACsec, eliminates the need for frequent secure association key (SAK) rekey that may occur in high capacity links (40 Gb/s, 100 Gb/s, and higher) and provides the option to use the GCM-AES-XPN-128 or GCM-AES-XPN-256 ciphersuites under the defined MKA policy.</td>
</tr>
<tr>
<td></td>
<td>128-bit—(Network Essentials and Network Advantage)</td>
</tr>
<tr>
<td></td>
<td>256-bit—(Network Advantage)</td>
</tr>
<tr>
<td>Network Address Translation (NAT) with scale enhancement</td>
<td>When configuring SDM templates for NAT usage, the maximum number of sessions that can be translated and forwarded in the hardware, in an ideal setting, is optimised to 14,000.</td>
</tr>
<tr>
<td></td>
<td>See IP → Configuring Network Address Translation.</td>
</tr>
<tr>
<td></td>
<td>(DNA Advantage)</td>
</tr>
<tr>
<td>Open Shortest Path First version 3 (OSPFv3) Authentication Trailer</td>
<td>Provides a mechanism to authenticate OSPFv3 protocol packets as an alternative to existing OSPFv3 IPsec authentication.</td>
</tr>
<tr>
<td></td>
<td>See Routing → Configuring OSPFv3 Authentication Trailer.</td>
</tr>
<tr>
<td></td>
<td>(Network Advantage)</td>
</tr>
</tbody>
</table>
The following programmability features are introduced in this release:

- **Application Hosting and IOx Support for Dockerized Applications**—A software as a service (SaaS) platform that allows Cisco applications and third party applications to run on the device. Hosted applications are supported within a Kernel Virtual Machine (KVM) and Linux Containers (LXC). Starting from Cisco IOS XE Fuji 16.9.1, Application Hosting supports Docker applications by running a Docker daemon within the customer-created IOx KVM guest operating system. (DNA Advantage)

- **Candidate Configuration**—A temporary configuration that can be modified without changing running configuration. You can then choose when to update the device’s configuration with the candidate configuration, by committing and confirming the candidate configuration.

- **OpenFlow 1.3 Multitable**—Enables integration with open source Faucet SDN Controllers to automate management of layer 2 switching, VLANs, ACLs, and layer 3 routing (Network Essentials and Network Advantage)

- **YANG Data Models**—For the list of Cisco IOS XE YANG models available with this release, navigate to https://github.com/YangModels.yang/tree/master/vendor/cisco/xe/1691. Revision statements embedded in the YANG files indicate if there has been a model revision. The README.md file in the same github location highlights changes that have been made in the release.

- **Zero Touch Provisioning (DHCPv6)**—Dynamic Host Control Protocol Version 6 (DHCPv6) support is added to the Zero-touch provisioning feature in this release. DHCPv6 is enabled by default, and works on any device that boots without startup configuration.

See Programmability Configuration Guide.
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description, License Level Information, Documentation Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Licensing</td>
<td>A cloud-based, software license management solution that allows you to manage and track the status of your license, hardware, and software usage trends.</td>
</tr>
</tbody>
</table>

**Note** Starting from this release, Smart Licensing is the default and the only available method to manage licenses.

**Important** Starting from Cisco IOS XE Fuji 16.9.1 the Right-To-Use (RTU) licensing mode is deprecated, and the associated `license right-to-use` command is no longer available on the CLI.

See the Smart Licensing, on page 36 section in this release note document.

A license level is not applicable.

<table>
<thead>
<tr>
<th>New on the Web UI</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>These features are introduced on the Web UI in this release</td>
<td>• Multicast—Minor improvements to configuring Internet Group Management Protocol (IGMP) snooping and to set the IGMP timeout.</td>
</tr>
<tr>
<td></td>
<td>• Open Shortest Path First (OSPF)—Supports OSPF standards-based routing protocol for improved routing of data packets to their destination.</td>
</tr>
<tr>
<td></td>
<td>• Quality of Service (QoS)—Supports QoS to make your network performance more predictable and bandwidth utilization more effective.</td>
</tr>
<tr>
<td></td>
<td>• Site Profile—New site profiles for access, distributed, and core switches for easier initial configuration of the device.</td>
</tr>
<tr>
<td></td>
<td>• Smart Licencing—Supports both online and offline method of license reservation to simplify and automate the management of licenses for your Cisco products. Smart Licensing on the device works with the Cisco Smart Software Manager (Cisco SSM).</td>
</tr>
<tr>
<td></td>
<td>• Switched Port Analyzer (SPAN)—Supports SPAN to analyze network traffic passing through ports or VLANs.</td>
</tr>
</tbody>
</table>
### Software Features Introduced on Cisco Catalyst 9500 Series Switches
(C9500-12Q, C9500-16X, C9500-24Q, C9500-40X)

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description, License Level Information, Documentation Link</th>
</tr>
</thead>
</table>
| AVC Switching: Export input and output interface information | • Support for two predefined directional wired Application Visibility and Control (WDAVC) Flexible NetFlow (FNF) records, ingress and egress, is introduced.  
• Support for attaching up to two different WDAVC FNF monitors with different records to an interface at the same time is enabled.  
See System Management → Configuring Application Visibility and Control in a Wired Network .  
(DNA Advantage)                                                                 |
| Blue Beacon                                       | The **show beacon all** privileged EXEC command is introduced; Use this command to display beacon LED status.  
See Interface and Hardware Commands .  
(Network Essentials and Network Advantage)         |
## Feature Name

<table>
<thead>
<tr>
<th>Description, License Level Information, Documentation Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco StackWise Virtual – Enhancement relating to supported ports</td>
</tr>
</tbody>
</table>
| Cisco StackWise Virtual was supported on a restricted number of ports on the Cisco Catalyst 9500 Series Switches. Starting from this release, this restriction has been removed and the feature can be configured on all the fixed ports of these models:  
  - C9500-24Q  
  - C9500-12Q  
  - C9500-40X  
  - C9500-16X |
| **Note** You still cannot configure Cisco StackWise Virtual links on the uplink (network) modules (C9500-NM-8X and C9500-NM-2Q). |
| See High Availability → Configuring Cisco StackWise Virtual |
| Also see these sections in this release note document for other important information about the feature:  
  - **Important Notes** → Cisco StackWise Virtual - Supported and Unsupported Features  
  - **Limitations and Restrictions** → Cisco StackWise Virtual |
| Display FPGA settings |
| The `show platform hardware fpga` privileged EXEC command is introduced; Use this command to display system Field Programmable Gate Arrays (FPGA) settings. |
| See System Management Commands . |
| Generic Online Diagnostics (GOLD) |
| The `TestUnusedPortLoopback` and `TestPortTxMonitoring` diagnostic test commands are introduced; Use these commands to test and verify the hardware functionality. |
| See System Management → Configuring Online Diagnostics .  
(Network Essentials and Network Advantage) |
### Feature Name | Description, License Level Information, Documentation Link
---|---
MACsec Key Agreement (MKA) cipher announcement exchange | Support for cipher announcement is enabled. Cipher Announcement allows the supplicant and the authenticator to announce their respective MACsec Cipher Suite capabilities through EAPoL announcements. Two types of EAPoL announcements are supported – Secured announcements and unsecured announcements.


128-bit—(Network Essentials and Network Advantage)
256-bit—(Network Advantage)

REP downlink support | Allows REP configuration on downlink ports.

See Layer 2 → Configuring Resilient Ethernet Protocol.

(Network Essentials and Network Advantage)

Virtual Extensible LAN (VXLAN) Border Gateway Protocol (BGP) Ethernet VPN (EVPN) | A VXLAN is a network overlay that allows layer 2 segments to be stretched across an IP core. All the benefits of layer 3 topologies are thereby available with VXLAN. The overlay protocol is VXLAN and BGP uses EVPN as the address family for communicating end host MAC and IP addresses

See Layer 2 → Configuring VXLAN BGP EVPN.

(Network Advantage)

### Software Features Introduced on Cisco Catalyst 9500 Series Switches-High Performance
(C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C)

| Feature Name | Description, License Level Information, Documentation Link |
---|---|
Boot Integrity Visibility | Allows Cisco's platform identity and software integrity information to be visible and actionable. Platform identity provides the platform’s manufacturing installed identity, and software integrity exposes boot integrity measurements that can be used to assess whether the platform has booted trusted code.

See System Management → Boot Integrity Visibility.

(Network Essentials and Network Advantage)
<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Description, License Level Information, Documentation Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabling MAC Address Learning on VLAN</td>
<td>The MAC address table contains address information that the switch uses to forward traffic between ports. All MAC addresses in the address table are associated with one or more ports. By default, MAC address learning is enabled on all interfaces and VLANs on the router. You can control MAC address learning on VLAN to manage the available MAC address table space by controlling which VLANs can learn the MAC addresses. Before you disable MAC address learning, be sure that you are familiar with the network topology and the router system configuration. Disabling MAC address learning on a VLAN could cause flooding in the network. See System Management → Administering the Device. (Network Essentials and Network Advantage)</td>
</tr>
<tr>
<td>Encapsulated Remote Switched Port Analyzer (ERSPAN)</td>
<td>ERSPAN enables you to monitor traffic on ports or VLANs and to send monitored traffic to destination ports. Starting with this release, the <strong>header-type 3</strong>, <strong>destination</strong>, <strong>sgt</strong>, <strong>dscp</strong>, and <strong>vrf</strong> ERSPAN monitor source session configuration mode commands are introduced. See Network Management → Configuring ERSPAN. (DNA Advantage)</td>
</tr>
<tr>
<td>Fast Unidirectional Link Detection (UDLD)</td>
<td>Enables subsecond UDLD. The UDLD protocol helps monitor a physical connection (such as monitoring wrong cabling) to detect unidirectional links to avoid spanning-tree topology loops or silent drop traffic. See Layer 2 → Configuring UniDirectional Link Detection. (Network Essentials and Network Advantage)</td>
</tr>
<tr>
<td>IPv6 Support for SGT and SGACL</td>
<td>Facilitates dynamic learning of mappings between IP addresses and Security Group Tags (SGTs) for IPv6 addresses. The SGT is then used to derive the Security Group Access Control List (SGACL). See Cisco TrustSec → IPv6 Support for SGT and SGACL. (Network Advantage)</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Description, License Level Information, Documentation Link</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Multiprotocol Label Switching | The following MPLS features are introduced in this release:  
  - EoMPLS—One of the Any Transport over MPLS (AToM) transport types. EoMPLS provides a tunneling mechanism for Ethernet traffic through an MPLS-enabled Layer 3 core. It encapsulates Ethernet protocol data units (PDUs) inside MPLS packets and uses label stacking to forward them across the MPLS network.  
  - VPLS—A class of VPN that supports the connection of multiple sites in a single bridged domain over a managed IP/MPLS network. VPLS uses the provider core to join multiple attachment circuits together, to simulate a virtual bridge that connects the multiple attachment circuits together.  
  - eBGP and iBGP—Enables you to configure multipath load balancing with both eBGP and iBGP paths in Border Gateway Protocol (BGP) networks that are configured to use MPLS VPNs. The feature provides improved load balancing deployment and service offering capabilities and is useful for multi-homed autonomous systems and Provider Edge (PE) routers that import both eBGP and iBGP paths from multihomed and stub networks.  

See [Multiprotocol Label Switching (MPLS)](Network Advantage) |
| SGT Name Export in NetFlow | Allows Flexible NetFlow to export Cisco TrustSec environmental data tables that map SGTs to Security Group Names.  

See [Cisco TrustSec → Flexible NetFlow Export of Cisco TrustSec Fields](DNA Essentials and DNA Advantage) |
| Top-N Reports | Enable you to collect and analyze data for each physical port on a switch. When Top-N reports start, they obtain statistics from the appropriate hardware counters and then go into sleep mode for a user-specified interval. When the interval ends, the reports obtain current statistics from the same hardware counters, compare current statistics with the earlier statistics, and store the difference.  

See [Network Management → Top-N Reports](Network Essentials and Network Advantage) |
**Important Notes**

- Cisco StackWise Virtual - Supported and Unsupported Features, on page 15
- Unsupported Features—All Models, on page 15
- Unsupported Features—Cisco Catalyst 9500 Series Switches, on page 15
- Unsupported Features—Cisco Catalyst 9500 Series Switches - High Performance, on page 16
- Complete List of Supported Features, on page 16
- Accessing Hidden Commands, on page 16

**Cisco StackWise Virtual - Supported and Unsupported Features**

(*applies only to C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models*)

When you enable Cisco StackWise Virtual on the device

- Layer 2, Layer 3, Security, Quality of Service, Multicast, Application, Monitoring and Management, Multiprotocol Label Switching, and High Availability are supported.

  Contact the Cisco Technical Support Centre for the specific list of features that are supported under each one of these technologies.

- Resilient Ethernet Protocol, Remote Switched Port Analyzer, and Software-Defined Access are NOT supported

**Unsupported Features—All Models**

- Bluetooth

- Bidirectional Protocol Independent Multicast (Bidir-PIM)

- Performance Monitoring (PerfMon)

- Virtual Routing and Forwarding (VRF)-Aware web authentication

**Unsupported Features—Cisco Catalyst 9500 Series Switches**

- Border Gateway Protocol (BGP) Additional Paths

- Cisco TrustSec Network Device Admission Control (NDAC) on Uplinks


- Gateway Load Balancing Protocol (GLBP)

- Lawful Intercept (LI)

- Network-Powered Lighting (including COAP Proxy Server, 2-event Classification, Perpetual POE, Fast PoE)

- PIM Bidirectional Forwarding Detection (PIM BFD), PIM Snooping.
• Quality of Service—Classification (Layer 3 Packet Length, Time-to-Live (TTL)), per queue policer support, sharped profile enablement for egress per port queues, L2 Miss, Ingress Packet FIFO (IPF)
• Unicast over Point to Multipoint (P2MP) Generic Routing Encapsulation (GRE), Multicast over P2MP GRE.
• VLAN Translation—One-to-One Mapping

Unsupported Features—Cisco Catalyst 9500 Series Switches - High Performance

• Cisco Application Visibility and Control (AVC)
• High Availability—Cisco Stackwise Virtual, Stateful Switchover (SSO), In Service Software Upgrade (ISSU), Nonstop Forwarding (NSF) (Enhanced Interior Gateway Routing Protocol (EIGRP) NSF and Open Shortest Path First (OSPF) NSF, NSF support for IPv6, NSF Awareness (BGP, EIGRP, OSPF))
• MPLS Label Distribution Protocol (MPLS LDP) VRF-Aware Static Labels
• Next Generation Network-Based Application Recognition (NBAR) and Next Generation NBAR (NBAR2)
• QoS Options on GRE Tunnel Interfaces

Complete List of Supported Features

For the complete list of features supported on a platform, see the Cisco Feature Navigator at https://www.cisco.com/go/cfn.

When you search for the list of features by platform select
• CAT9500—to see all the features supported on the C9500-12Q, C9500-16X, C9500-24Q, C9500-40X models
• CAT9500 HIGH PERFORMANCE (32C; 32QC; 48Y4C; 24Y4C)—to see all the features supported on the C9500-24Y4C, C9500-32C, C9500-32QC, and C9500-48Y4C models

Accessing Hidden Commands

Starting with Cisco IOS XE Fuji 16.8.1a, as an improved security measure, the way in which hidden commands can be accessed has changed.

Hidden commands have always been present in Cisco IOS XE, but were not equipped with CLI help. This means that entering enter a question mark (?) at the system prompt did not display the list of available commands. For information about CLI help, see Understanding the Help System. Such hidden commands are only meant to assist Cisco TAC in advanced troubleshooting and are therefore not documented.

Starting with Cisco IOS XE Fuji 16.8.1a, hidden commands are available under:
• Category 1—Hidden commands in privileged or User EXEC mode. Begin by entering the service internal command to access these commands.
• Category 2—Hidden commands in one of the configuration modes (global, interface and so on). These commands do not require the service internal command.

Further, the following applies to hidden commands under Category 1 and 2:
• The commands have CLI help. Entering enter a question mark (?) at the system prompt displays the list of available commands.
Note: For Category 1, enter the service internal command before you enter the question mark; you do not have to do this for Category 2.

• The system generates a %PARSER-5-HIDDEN syslog message when the command is used. For example:
  
  *Feb 14 10:44:37.917: %PARSER-5-HIDDEN: Warning!!! 'show processes memory old-header ' is a hidden command.
  Use of this command is not recommended/supported and will be removed in future.

Apart from category 1 and 2, there remain internal commands displayed on the CLI, for which the system does NOT generate the %PARSER-5-HIDDEN syslog message.

---

**Important**

We recommend that you use any hidden command only under TAC supervision.

If you find that you are using a hidden command, open a TAC case for help with finding another way of collecting the same information as the hidden command (for a hidden EXEC mode command), or to configure the same functionality (for a hidden configuration mode command) using non-hidden commands.

---

**Supported Hardware**

**Cisco Catalyst 9500 Series Switches—Model Numbers**

The following table lists the supported hardware models and the default license levels they are delivered with. For information about the available license levels, see section *License Levels*.

The Base PIDs are the model numbers of the switch.

The Bundled PIDs indicate the orderable part numbers for base PIDs that are bundled with a particular network module; entering the `show version`, `show module`, or `show inventory` command on such a switch (bundled PID), displays its base PID.

**Table 1: Cisco Catalyst 9500 Series Switches**

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Default License Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base PIDs</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C9500-12Q-E</td>
<td>Network Essentials</td>
<td>12 40-Gigabit Ethernet QSFP+ ports and two power supply slots</td>
</tr>
<tr>
<td>C9500-12Q-A</td>
<td>Network Advantage</td>
<td></td>
</tr>
<tr>
<td>C9500-16X-E</td>
<td>Network Essentials</td>
<td>16 1/10-Gigabit Ethernet SFP/SFP+ ports and two power supply slots</td>
</tr>
<tr>
<td>C9500-16X-A</td>
<td>Network Advantage</td>
<td></td>
</tr>
<tr>
<td>C9500-24Q-E</td>
<td>Network Essentials</td>
<td>24-Port 40-Gigabit Ethernet QSFP+ ports and two power supply slots</td>
</tr>
<tr>
<td>C9500-24Q-A</td>
<td>Network Advantage</td>
<td></td>
</tr>
<tr>
<td>C9500-40X-E</td>
<td>Network Essentials</td>
<td>40 1/10-Gigabit Ethernet SFP/SFP+ ports and two power supply slots</td>
</tr>
<tr>
<td>C9500-40X-A</td>
<td>Network Advantage</td>
<td></td>
</tr>
</tbody>
</table>
### Table 1: Bundled PIDs

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Default License Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C9500-16X-2Q-E</td>
<td>Network Essentials</td>
<td>16 10-Gigabit Ethernet SFP+ port switch and a 2-Port 40-Gigabit Ethernet (QSFP) network module on uplink ports</td>
</tr>
<tr>
<td>C9500-16X-2Q-A</td>
<td>Network Advantage</td>
<td></td>
</tr>
<tr>
<td>C9500-24X-E</td>
<td>Network Essentials</td>
<td>16 10-Gigabit Ethernet SFP+ port switch and an 8-Port 10-Gigabit Ethernet (SFP) network module on uplink ports</td>
</tr>
<tr>
<td>C9500-24X-A</td>
<td>Network Advantage</td>
<td></td>
</tr>
<tr>
<td>C9500-40X-2Q-E</td>
<td>Network Essentials</td>
<td>40 10-Gigabit Ethernet SFP+ port switch and a 2-Port 40-Gigabit Ethernet (QSFP) network module on uplink ports</td>
</tr>
<tr>
<td>C9500-40X-2Q-A</td>
<td>Network Advantage</td>
<td></td>
</tr>
<tr>
<td>C9500-48X-E</td>
<td>Network Essentials</td>
<td>40 10-Gigabit Ethernet SFP+ port switch and an 8-Port 10-Gigabit Ethernet (SFP) network module on uplink ports</td>
</tr>
<tr>
<td>C9500-48X-A</td>
<td>Network Advantage</td>
<td></td>
</tr>
</tbody>
</table>

1 See section Licensing → Table: Permitted Combinations, in this document for information about the add-on licenses that you can order.

### Table 2: Cisco Catalyst 9500 Series Switches—High Performance

<table>
<thead>
<tr>
<th>Switch Model</th>
<th>Default License Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C9500-24Y4C-E</td>
<td>Network Essentials</td>
<td>24 SFP28 ports that support 1/10/25-GigabitEthernet connectivity, four QSFP uplink ports that support 100/40-GigabitEthernet connectivity; two power supply slots.</td>
</tr>
<tr>
<td>C9500-24Y4C-A</td>
<td>Network Advantage</td>
<td></td>
</tr>
<tr>
<td>C9500-32C-E</td>
<td>Network Essentials</td>
<td>32 QSFP28 ports that support 40/100 GigabitEthernet connectivity; two power supply slots.</td>
</tr>
<tr>
<td>C9500-32C-A</td>
<td>Network Advantage</td>
<td></td>
</tr>
<tr>
<td>C9500-32QC-E</td>
<td>Network Essentials</td>
<td>32 QSFP28 ports, where you can have 24 ports that support 40-GigabitEthernet connectivity and 4 ports that support 100-GigabitEthernet connectivity, OR 32 ports that support 40-GigabitEthernet connectivity, OR 16 ports that support 100-GigabitEthernet connectivity; two power supply slots.</td>
</tr>
<tr>
<td>C9500-32QC-A</td>
<td>Network Advantage</td>
<td></td>
</tr>
<tr>
<td>C9500-48Y4C-E</td>
<td>Network Essentials</td>
<td>48 SFP28 ports that support 1/10/25-GigabitEthernet connectivity; four QSFP uplink ports that supports up to 100/40-GigabitEthernet connectivity; two power supply slots.</td>
</tr>
<tr>
<td>C9500-48Y4C-A</td>
<td>Network Advantage</td>
<td></td>
</tr>
</tbody>
</table>

2 See section Licensing → Table: Permitted Combinations, in this document for information about the add-on licenses that you can order.
Network Modules

The following table lists optional network modules for uplink ports available with some configurations.

<table>
<thead>
<tr>
<th>Network Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C9500-NM-8X</td>
<td>Cisco Catalyst 9500 Series Network Module 8-port 1/10 Gigabit Ethernet with SFP/SFP+</td>
</tr>
<tr>
<td></td>
<td>Note the supported switch models (Base PIDs):</td>
</tr>
<tr>
<td></td>
<td>• C9500-40X</td>
</tr>
<tr>
<td></td>
<td>• C9500-16X</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Module</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>C9500-NM-2Q</td>
<td>Cisco Catalyst 9500 Series Network Module 2-port 40 Gigabit Ethernet with QSFP+</td>
</tr>
<tr>
<td></td>
<td>Note the supported switch models (Base PIDs):</td>
</tr>
<tr>
<td></td>
<td>• C9500-40X</td>
</tr>
<tr>
<td></td>
<td>• C9500-16X</td>
</tr>
</tbody>
</table>

Optics Modules

Cisco Catalyst Series Switches support a wide range of optics and the list of supported optics is updated on a regular basis. Use the Transceiver Module Group (TMG) Compatibility Matrix tool, or consult the tables at this URL for the latest transceiver module compatibility information: https://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

Compatibility Matrix

The following table provides software compatibility information.

<table>
<thead>
<tr>
<th>Catalyst 9500 and 9500-High Performance</th>
<th>Cisco Identity Services Engine</th>
<th>Cisco Access Control Server</th>
<th>Cisco Prime Infrastructure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fuji 16.9.2</td>
<td>2.3 Patch 1</td>
<td>5.4</td>
<td>PI 3.4 + PI 3.4 latest maintenance release + PI 3.4 latest device pack</td>
</tr>
<tr>
<td></td>
<td>2.4 Patch 1</td>
<td>5.5</td>
<td>See Cisco Prime Infrastructure 3.4→ Downloads.</td>
</tr>
<tr>
<td>Fuji 16.9.1</td>
<td>2.3 Patch 1</td>
<td>5.4</td>
<td>PI 3.4 + PI 3.4 latest device pack</td>
</tr>
<tr>
<td></td>
<td>2.4 Patch 1</td>
<td>5.5</td>
<td>See Cisco Prime Infrastructure 3.4→ Downloads.</td>
</tr>
</tbody>
</table>
Web UI System Requirements

The following subsections list the hardware and software required to access the Web UI:

Minimum Hardware Requirements

<table>
<thead>
<tr>
<th>Processor Speed</th>
<th>DRAM</th>
<th>Number of Colors</th>
<th>Resolution</th>
<th>Font Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>233 MHz minimum</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 GHz minimum</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1 We recommend 1 GHz

2 We recommend 1 GB DRAM
Software Requirements

Operating Systems

• Windows 10 or later
• Mac OS X 10.9.5 or later

Browsers

• Google Chrome—Version 59 or later (On Windows and Mac)
• Microsoft Edge
• Mozilla Firefox—Version 54 or later (On Windows and Mac)
• Safari—Version 10 or later (On Mac)

Upgrading the Switch Software

This section covers the various aspects of upgrading or downgrading the device software.

Note
You cannot use the Web UI to install, upgrade, or downgrade device software.

Finding the Software Version

The package files for the Cisco IOS XE software are stored on the system board flash device (flash:).

You can use the `show version` privileged EXEC command to see the software version that is running on your switch.

Note
Although the `show version` output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration and does not change if you upgrade the software license.

You can also use the `dir filesystem:` privileged EXEC command to see the directory names of other software images that you might have stored in flash memory.

Software Images

<table>
<thead>
<tr>
<th>Release</th>
<th>Image Type</th>
<th>File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>CAT9K_IOSXE</td>
<td>cat9k_iosxe.16.09.01.SPA.bin</td>
</tr>
<tr>
<td></td>
<td>Licensed Data Payload Encryption (LDPE)</td>
<td>cat9k_iosxeldpe.16.09.01.SPA.bin</td>
</tr>
</tbody>
</table>
Automatic Boot Loader Upgrade

When you upgrade from the existing release on your switch to a later or newer release for the first time, the boot loader may be automatically upgraded, based on the hardware version of the switch. If the boot loader is automatically upgraded, it will take effect on the next reload. If you go back to the older release after this, the boot loader is not downgraded. The updated boot loader supports all previous releases.

For subsequent Cisco IOS XE Everest 16.x.x, or Cisco IOS XE Fuji 16.x.x releases, if there is a new bootloader in that release, it may be automatically upgraded based on the hardware version of the switch when you boot up your switch with the new image for the first time.

⚠️ Caution

Do not power cycle your switch during the upgrade.

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Automatic Boot Loader Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>If you boot Cisco IOS XE Fuji 16.9.1 first time</td>
<td>On Cisco Catalyst 9500 Series Switches, the boot loader may be upgraded to version 16.9.1r [FC2]. For example:</td>
</tr>
<tr>
<td></td>
<td>ROM: IOS-XE ROMMON</td>
</tr>
<tr>
<td></td>
<td>BOOTLDR: System Bootstrap, Version 16.9.1r [FC2], RELEASE SOFTWARE (P)</td>
</tr>
<tr>
<td></td>
<td>If you boot Cisco IOS XE Fuji 16.9.1, you will see the following on the console:</td>
</tr>
<tr>
<td></td>
<td>&quot;!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!&quot;</td>
</tr>
<tr>
<td></td>
<td>%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): ### Thu Jul 5 18:03:28 Universal 2018 PLEASE DO NOT POWER CYCLE ###</td>
</tr>
<tr>
<td></td>
<td>BOOT LOADER UPGRADING</td>
</tr>
<tr>
<td></td>
<td>waiting for upgrades to complete...</td>
</tr>
<tr>
<td></td>
<td>On Cisco Catalyst 9500 Series Switches - High Performance, the boot loader may be upgraded to version 16.9.1r [FC3]. For example:</td>
</tr>
<tr>
<td></td>
<td>ROM: IOS-XE ROMMON</td>
</tr>
<tr>
<td></td>
<td>BOOTLDR: System Bootstrap, Version 16.9.1r [FC3], RELEASE SOFTWARE (P)</td>
</tr>
<tr>
<td></td>
<td>If the automatic boot loader upgrade occurs, while booting Cisco IOS XE Fuji 16.9.1, you will see the following on the console:</td>
</tr>
<tr>
<td></td>
<td>&quot;!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!&quot;</td>
</tr>
<tr>
<td></td>
<td>%IOSXEBOOT-4-BOOTLOADER_UPGRADE: (rp/0): ### Thu Jul 5 18:03:28 Universal 2018 PLEASE DO NOT POWER CYCLE ###</td>
</tr>
<tr>
<td></td>
<td>BOOT LOADER UPGRADING</td>
</tr>
<tr>
<td></td>
<td>waiting for upgrades to complete...</td>
</tr>
</tbody>
</table>

Software Installation Commands

⚠️ Note

The request platform software commands are deprecated starting from Cisco IOS XE Gibraltar 16.10.1. The commands are visible on the CLI in this release and you can configure them, but we recommend that you use the install commands to upgrade or downgrade.

<table>
<thead>
<tr>
<th>Note</th>
<th>This table of commands is not supported on Cisco Catalyst 9500 Series Switches - High Performance.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device# request platform software package ?</td>
<td></td>
</tr>
<tr>
<td>clean</td>
<td>Cleans unnecessary package files from media</td>
</tr>
</tbody>
</table>
This table of commands is not supported on Cisco Catalyst 9500 Series Switches - High Performance.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>copy</td>
<td>Copies package to media</td>
</tr>
<tr>
<td>describe</td>
<td>Describes package content</td>
</tr>
<tr>
<td>expand</td>
<td>Expands all-in-one package to media</td>
</tr>
<tr>
<td>install</td>
<td>Installs the package</td>
</tr>
<tr>
<td>uninstall</td>
<td>Uninstalls the package</td>
</tr>
<tr>
<td>verify</td>
<td>Verifies In Service Software Upgrade (ISSU) software package compatibility</td>
</tr>
</tbody>
</table>

Cisco IOS XE Everest 16.6.2 and later releases

To install and activate the specified file, and to commit changes to be persistent across reloads—Device#
install add file filename [activate commit]

To separately install, activate, commit, abort, or remove the installation file—Device# install ?

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add file tftp: filename</td>
<td>Copies the install file package from a remote location to the device and performs a compatibility check for the platform and image versions.</td>
</tr>
<tr>
<td>activate [auto-abort-timer]</td>
<td>Activates the file, and reloads the device. The auto-abort-timer keyword automatically rolls back image activation.</td>
</tr>
<tr>
<td>commit</td>
<td>Makes changes persistent over reloads.</td>
</tr>
<tr>
<td>rollback to committed</td>
<td>Rolls back the update to the last committed version.</td>
</tr>
<tr>
<td>abort</td>
<td>Aborts file activation, and rolls back to the version that was running before the current installation procedure started.</td>
</tr>
<tr>
<td>remove</td>
<td>Deletes all unused and inactive software installation files.</td>
</tr>
</tbody>
</table>

Upgrading in Install Mode

Follow these instructions to upgrade from one release to another, in install mode. To perform a software image upgrade, you must be booted into IOS through boot flash:packages.conf

Before you begin

Note that you can use this procedure for the following upgrade scenarios:
To upgrade to... Use these commands... To upgrade to...

<table>
<thead>
<tr>
<th>When upgrading from ...</th>
<th>Use these commands...</th>
<th>To upgrade to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Everest 16.5.1a or Cisco IOS XE Everest 16.6.1</td>
<td>Only request platform software commands</td>
<td>Cisco IOS XE Fuji 16.9.1</td>
</tr>
<tr>
<td>Cisco IOS XE Everest 16.6.2 and later</td>
<td>On Cisco Catalyst 9500 Series Switches either install commands or request platform software commands</td>
<td>Cisco IOS XE Everest 16.6.2 and later</td>
</tr>
</tbody>
</table>

5 Introduced in Cisco IOS XE Fuji 16.8.1a

The sample output in this section displays upgrade from

- Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Fuji 16.9.1 using request platform software commands.
- Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Fuji 16.9.1 using install commands.

Procedure

Step 1 Clean Up

Ensure that you have at least 1GB of space in flash to expand a new image. Clean up old installation files in case of insufficient space.

- request platform software package clean
- install remove inactive

The following sample output displays the cleaning up of unused files, by using the request platform software package clean command for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Fuji 16.9.1.

Switch# request platform software package clean
Running command on switch 1
Cleaning up unnecessary package files
No path specified, will use booted path flash:packages.conf
Cleaning flash:
Scanning boot directory for packages ... done.
Preparing packages list to delete ...
cat9k-cc_srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-espbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-guestshell.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-rpboot.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipbase.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-sipspa.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-srdriver.16.05.01a.SPA.pkg
File is in use, will not delete.
cat9k-webui.16.05.01a.SPA.pkg
The following sample output displays the cleaning up of unused files, by using the `install remove inactive` command, for upgrade scenario Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Fuji 16.9.1:

```
Switch# install remove inactive
install_remove: START Tue Jul 10 19:51:48 UTC 2017
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ... done.

The following files will be deleted:
[switch 1]:
  /flash/cat9k-cc_srdriver.16.06.01.SPA.pkg
  /flash/cat9k-espbase.16.06.01.SPA.pkg
  /flash/cat9k-guestshell.16.06.01.SPA.pkg
  /flash/cat9k-rpbase.16.06.01.SPA.pkg
  /flash/cat9k-sipbase.16.06.01.SPA.pkg
  /flash/cat9k-sipspa.16.06.01.SPA.pkg
  /flash/cat9k-rpboot.16.06.01.SPA.pkg
  /flash/cat9k-iosxe.16.06.01.SPA.pkg
  /flash/packages.conf.00-
  /flash/packages.conf
```

Switch#
Do you want to remove the above files? [y/n] y

[switch 1]:
Removing file flash:cat9k-cc_srdriver.16.06.03.SPA.pkg ... done.
Removing file flash:cat9k-espbase.16.06.03.SPA.pkg ... done.
Removing file flash:cat9k-guestshell.16.06.03.SPA.pkg ... done.
Removing file flash:cat9k-rpbase.16.06.03.SPA.pkg ... done.
Removing file flash:cat9k-rpboot.16.06.03.SPA.pkg ... done.
Removing file flash:cat9k-sipbase.16.06.03.SPA.pkg ... done.
Removing file flash:cat9k-sipspa.16.06.03.SPA.pkg ... done.
Removing file flash:cat9k-srdriver.16.06.03.SPA.pkg ... done.
Removing file flash:cat9k-webui.16.06.03.SPA.pkg ... done.
Removing file flash:packages.conf ... done.
SUCCESS: Files deleted.

--- Starting Post_Remove_Cleanup ---
Performing Post_Remove_Cleanup on all members
[1] Post_Remove_Cleanup package(s) on switch 1
[1] Finished Post_Remove_Cleanup on switch 1
Checking status of Post_Remove_Cleanup on [1]
Post_Remove_Cleanup: Passed on [1]
Finished Post_Remove_Cleanup
SUCCESS: install_remove Tue Jul 10 19:52:25 UTC 2018
Switch#

Step 2  Copy new image to flash

a)  copy tftp: flash:

    Use this command to copy the new image to flash: (or skip this step if you want to use the new image
    from your TFTP server)

Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.09.01.SPA.bin flash:

    Destination filename [cat9k_iosxe.16.09.01.SPA.bin]?
    Accessing tftp://10.8.0.6//cat9k_iosxe.16.09.01.SPA.bin...
    Loading /cat9k_iosxe.16.09.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):
    !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
    [OK - 60126545 bytes]

    60126545 bytes copied in 50.649 secs (11870255 bytes/sec)

b)  dir flash

    Use this command to confirm that the image has been successfully copied to flash.

Switch# dir flash:/*.bin
Directory of flash:/*.bin

    Directory of flash:

    434184 -rw- 60126545 Jul 10 2018 10:18:11 -07:00 cat9k_iosxe.16.09.01.SPA.bin
    11353194496 bytes total (8976625664 bytes free)

Step 3  Software install image to flash

    • request platform software package install
    • install add file activate commit
The following sample output displays installation of the Cisco IOS XE Fuji 16.9.1 software image to flash, by using the request platform software package install command, for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Fuji 16.9.1.

Switch# request platform software package install switch all file flash:cat9k_iosxe.16.09.01.SPA.bin

--- Starting install local lock acquisition on switch 1 ---
Finished install local lock acquisition on switch 1

Expanding image file: flash:cat9k_iosxe.16.09.01.SPA.bin
[1]: Finished copying to switch
[1]: Expanding file
[1]: Finished expanding all-in-one software package in switch 1
SUCCESS: Finished expanding all-in-one software package.
[1]: Performing install
SUCCESS: install finished
[1]: install package(s) on switch 1
--- Starting list of software package changes ---
Old files list:
Removed cat9k-cc_srdriver.16.05.01a.SPA.pkg
Removed cat9k-espbase.16.05.01a.SPA.pkg
Removed cat9k-guestshell.16.05.01a.SPA.pkg
Removed cat9k-rpbase.16.05.01a.SPA.pkg
Removed cat9k-rpboot.16.05.01a.SPA.pkg
Removed cat9k-slipbase.16.05.01a.SPA.pkg
Removed cat9k-sipspa.16.05.01a.SPA.pkg
Removed cat9k-srdriver.16.05.01a.SPA.pkg
Removed cat9k-webui.16.05.01a.SPA.pkg
Removed cat9k-wlc.16.05.01a.SPA.pkg
New files list:
Added cat9k-cc_srdriver.16.09.01.SPA.pkg
Added cat9k-espbase.16.09.01.SPA.pkg
Added cat9k-guestshell.16.09.01.SPA.pkg
Added cat9k-rpbase.16.09.01.SPA.pkg
Added cat9k-rpboot.16.09.01.SPA.pkg
Added cat9k-slipbase.16.09.01.SPA.pkg
Added cat9k-sipspa.16.09.01.SPA.pkg
Added cat9k-srdriver.16.09.01.SPA.pkg
Added cat9k-webui.16.09.01.SPA.pkg
Finished list of software package changes
SUCCESS: Software provisioned. New software will load on reboot.

[1]: Finished install successful on switch 1
Checking status of install on [1]
[1]: Finished install in switch 1
SUCCESS: Finished install: Success on [1]

Note: Old files listed in the logs are not removed from flash.

The following sample output displays installation of the Cisco IOS XE Fuji 16.9.1 software image to flash, by using the install add file activate commit command, for upgrade scenario Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Fuji 16.9.1:

Switch# install add file flash:cat9k_iosxe.16.09.01.SPA.bin activate commit

install_add_activate_commit: START Tue Jul 10 19:54:51 UTC 2018
System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]?y
Building configuration...
Modified configuration has been saved

*Mar 16 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 10 19:54:55 install_engine.sh:

%INSTALL-5-INSTALL_START_INFO: Started install one-shot
flash:cat9k_iosxe.16.09.01.SPA.bininstall_add_activate_commit: Adding PACKAGE

This operation requires a reload of the system. Do you want to proceed?
Please confirm you have changed boot config to flash:packages.conf[y/n]y

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.16.09.01.SPA.bin to the selected switch(es)
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
[1] Add package(s) on switch 1
[1] Finished Add on switch 1
Checking status of Add on [1]
Add: Passed on [1]
Finished Add

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
/flash/cat9k-wlc.16.09.01.SPA.pkg
/flash/cat9k-webui.16.09.01.SPA.pkg
/flash/cat9k-srdriver.16.09.01.SPA.pkg
/flash/cat9k-sipspa.16.09.01.SPA.pkg
/flash/cat9k-sipbase.16.09.01.SPA.pkg
/flash/cat9k-rpboot.16.09.01.SPA.pkg
/flash/cat9k-rpbase.16.09.01.SPA.pkg
/flash/cat9k-guestshell.16.09.01.SPA.pkg
/flash/cat9k-espbase.16.09.01.SPA.pkg
/flash/cat9k-cc_srdriver.16.09.01.SPA.pkg

This operation requires a reload of the system. Do you want to proceed?[y/n]y
--- Starting Activate ---
Performing Activate on all members
[1] Activate package(s) on switch 1
[1] Finished Activate on switch 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

--- Starting Commit ---
Performing Commit on all members

*Mar 16 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 10 19:57:41 rollback_timer.sh:

%INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Install auto abort timer will expire in 7200
seconds [1] Commit package(s) on switch 1
[1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit Tue Jul 10 19:57:48 UTC 2018
Switch#

**Note** The system reloads automatically after executing the install add file activate commit command. You do not have to manually reload the system.
Step 4  
**dir flash:**

After the software has been successfully installed, use this command to verify that the flash partition has ten new `.pkg` files and three `.conf` files.

The following is sample output of the `dir flash:` command for upgrade scenario Cisco IOS XE Everest 16.5.1a to Cisco IOS XE Fuji 16.9.1:

```
Switch# dir flash:*.pkg
Directory of flash:/*.pkg
Directory of flash:/
475140 -rw- 2012104 Jul 26 2017 09:52:41 -07:00 cat9k-cc_srdriver.16.05.01a.SPA.pkg
475141 -rw- 70333380 Jul 26 2017 09:52:44 -07:00 cat9k-espbase.16.05.01a.SPA.pkg
475142 -rw- 13256 Jul 26 2017 09:52:44 -07:00 cat9k-guestshell.16.05.01a.SPA.pkg
475143 -rw- 349635524 Jul 26 2017 09:52:54 -07:00 cat9k-rpbase.16.05.01a.SPA.pkg
475149 -rw- 24248187 Jul 26 2017 09:53:02 -07:00 cat9k-rpboot.16.05.01a.SPA.pkg
475144 -rw- 25285572 Jul 26 2017 09:52:55 -07:00 cat9k-sipbase.16.05.01a.SPA.pkg
475145 -rw- 20947908 Jul 26 2017 09:52:56 -07:00 cat9k-sipspa.16.05.01a.SPA.pkg
475146 -rw- 2392372 Jul 26 2017 09:52:56 -07:00 cat9k-srdriver.16.05.01a.SPA.pkg
475147 -rw- 13282488 Jul 26 2017 09:52:56 -07:00 cat9k-webui.16.05.01a.SPA.pkg
475148 -rw- 13248 Jul 26 2017 09:52:56 -07:00 cat9k-wlc.16.05.01a.SPA.pkg
491524 -rw- 25711568 Jul 10 2018 11:49:33 -07:00 cat9k-cc_srdriver.16.09.01.SPA.pkg
491525 -rw- 78484428 Jul 10 2018 11:49:35 -07:00 cat9k-espbase.16.09.01.SPA.pkg
491526 -rw- 1598412 Jul 10 2018 11:49:35 -07:00 cat9k-guestshell.16.09.01.SPA.pkg
491527 -rw- 404153288 Jul 10 2018 11:49:47 -07:00 cat9k-rpbase.16.09.01.SPA.pkg
491533 -rw- 31657374 Jul 10 2018 11:50:09 -07:00 cat9k-rpboot.16.09.01.SPA.pkg
491528 -rw- 27681740 Jul 10 2018 11:49:48 -07:00 cat9k-sipbase.16.09.01.SPA.pkg
491529 -rw- 52224968 Jul 10 2018 11:49:49 -07:00 cat9k-sipspa.16.09.01.SPA.pkg
491530 -rw- 31130572 Jul 10 2018 11:49:50 -07:00 cat9k-srdriver.16.09.01.SPA.pkg
491531 -rw- 14783432 Jul 10 2018 11:49:51 -07:00 cat9k-webui.16.09.01.SPA.pkg
491532 -rw- 9160 Jul 10 2018 11:49:51 -07:00 cat9k-wlc.16.09.01.SPA.pkg

11353194496 bytes total (8963174400 bytes free)
```

The following is sample output of the `dir flash:` command for the Cisco IOS XE Everest 16.6.3 to Cisco IOS XE Fuji 16.9.1 upgrade scenario:

```
Switch# dir flash:
Directory of flash: /
475140 -rw- 2012104 Jul 26 2017 09:52:41 -07:00 cat9k-cc_srdriver.16.06.03.SPA.pkg
475141 -rw- 70333380 Jul 26 2017 09:52:44 -07:00 cat9k-espbase.16.06.03.SPA.pkg
475142 -rw- 13256 Jul 26 2017 09:52:44 -07:00 cat9k-guestshell.16.06.03.SPA.pkg
475143 -rw- 349635524 Jul 26 2017 09:52:54 -07:00 cat9k-rpbase.16.06.03.SPA.pkg
475149 -rw- 24248187 Jul 26 2017 09:53:02 -07:00 cat9k-rpboot.16.06.03.SPA.pkg
475144 -rw- 25285572 Jul 26 2017 09:52:55 -07:00 cat9k-sipbase.16.06.03.SPA.pkg
475145 -rw- 20947908 Jul 26 2017 09:52:56 -07:00 cat9k-sipspa.16.06.03.SPA.pkg
475146 -rw- 2392372 Jul 26 2017 09:52:56 -07:00 cat9k-srdriver.16.06.03.SPA.pkg
475147 -rw- 13284288 Jul 26 2017 09:52:56 -07:00 cat9k-webui.16.06.03.SPA.pkg
475148 -rw- 13248 Jul 26 2017 09:52:56 -07:00 cat9k-wlc.16.06.03.SPA.pkg
491524 -rw- 25711568 Jul 10 2018 11:49:33 -07:00 cat9k-cc_srdriver.16.09.01.SPA.pkg
491525 -rw- 78484428 Jul 10 2018 11:49:35 -07:00 cat9k-espbase.16.09.01.SPA.pkg
491526 -rw- 1598412 Jul 10 2018 11:49:35 -07:00 cat9k-guestshell.16.09.01.SPA.pkg
491527 -rw- 404153288 Jul 10 2018 11:49:47 -07:00 cat9k-rpbase.16.09.01.SPA.pkg
491533 -rw- 31657374 Jul 10 2018 11:50:09 -07:00 cat9k-rpboot.16.09.01.SPA.pkg
491528 -rw- 27681740 Jul 10 2018 11:49:48 -07:00 cat9k-sipbase.16.09.01.SPA.pkg
491529 -rw- 52224968 Jul 10 2018 11:49:49 -07:00 cat9k-sipspa.16.09.01.SPA.pkg
491530 -rw- 31130572 Jul 10 2018 11:49:50 -07:00 cat9k-srdriver.16.09.01.SPA.pkg
491531 -rw- 14783432 Jul 10 2018 11:49:51 -07:00 cat9k-webui.16.09.01.SPA.pkg
491532 -rw- 9160 Jul 10 2018 11:49:51 -07:00 cat9k-wlc.16.09.01.SPA.pkg

11353194496 bytes total (8963174400 bytes free)
```
The following sample output displays the .conf files in the flash partition; note the three .conf files:

- packages.conf—the file that has been re-written with the newly installed .pkg files
- packages.conf.00—backup file of the previously installed image
- cat9k_iosxe.16.09.01.SPA.conf—a copy of packages.conf and not used by the system.

```
Switch# dir flash:*.conf
Directory of flash:/*.conf
Directory of flash:/
434197 -rw- 7406 Jul 10 2018 10:59:16 -07:00 packages.conf
434196 -rw- 7504 Jul 10 2018 10:59:16 -07:00 packages.conf.00-
516098 -rw- 7406 Jul 10 2018 10:58:08 -07:00 cat9k_iosxe.16.09.01.SPA.conf
11353194496 bytes total (8963174400 bytes free)
```

**Step 5**  
Reload  

a) **reload**

Use this command to reload the switch.

```
Switch# reload
```

b) **boot flash:**

If your switches are configured with auto boot, then the stack will automatically boot up with the new image. If not, you can manually boot flash:packages.conf

```
Switch: boot flash:packages.conf
```

c) **show version**

After the image boots up, use this command to verify the version of the new image.

**Note**  
When you boot the new image, the boot loader is automatically updated, but the new bootloader version is not displayed in the output until the next reload.

The following sample output of the **show version** command displays the Cisco IOS XE Fuji 16.9.1 image on the device:

```
Switch# show version
Cisco IOS XE Software, Version 16.09.01

Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.9.1,
RELEASE SOFTWARE (fc1)  
Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2018 by Cisco Systems, Inc.
```
Downgrading in Install Mode

Follow these instructions to downgrade from one release to another, in install mode. To perform a software image downgrade, you must be booted into IOS via “boot flash:packages.conf.”

Before you begin

Note that you can use this procedure for the following downgrade scenarios:

<table>
<thead>
<tr>
<th>When downgrading from...</th>
<th>Use these commands...</th>
<th>To downgrade to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS XE Fuji 16.9.1</td>
<td>On Cisco Catalyst 9500 Series Switches, either install commands or request platform software commands</td>
<td>Cisco IOS XE Fuji 16.8.x or Cisco IOS XE Everest 16.x.x release.</td>
</tr>
<tr>
<td></td>
<td>On Cisco Catalyst 9500 Series Switches - High Performance, only install commands</td>
<td></td>
</tr>
</tbody>
</table>

6 Introduced in Cisco IOS XE Fuji 16.8.1a

The sample output in this section shows downgrade from Cisco IOS XE Fuji 16.9.1 to Cisco IOS XE Everest 16.6.1, by using the install commands.

Important

New switch models that are introduced in a release cannot be downgraded. For instance, if a new model is first introduced in Cisco IOS XE Fuji 16.8.1a, this is the minimum software version for the model.

Procedure

Step 1 Clean Up

Ensure that you have at least 1GB of space in flash to expand a new image. Clean up old installation files in case of insufficient space.

- install remove inactive
- request platform software package clean

The following sample output displays the cleaning up of Cisco IOS XE Fuji 16.9.1 files using the install remove inactive command:

Switch# install remove inactive

install_remove: START Tue Jul 10 19:51:48 UTC 2018
Cleaning up unnecessary package files
Scanning boot directory for packages ... done.
Preparing packages list to delete ... done.

The following files will be deleted:
Step 2  Copy new image to flash

a)  copy tftp: flash:

Use this command to copy the new image to flash: (or skip this step if you want to use the new image from your TFTP server)

Switch# copy tftp://10.8.0.6//cat9k_iosxe.16.06.01.SPA.bin flash:

Destination filename [cat9k_iosxe.16.06.01.SPA.bin]?

Accessing tftp://10.8.0.6//cat9k_iosxe.16.06.01.SPA.bin...

Loading /cat9k_iosxe.16.06.01.SPA.bin from 10.8.0.6 (via GigabitEthernet0/0):

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 508584771 bytes]

508584771 bytes copied in 101.005 secs (5035244 bytes/sec)

b)  dir flash:

Use this command to confirm that the image has been successfully copied to flash.

Switch# dir flash:/*.bin
Directory of flash:/*.bin

Directory of flash:
Step 3  
**Downgrade software image**

- `install add file activate commit`
- `request platform software package install`

The following example displays the installation of the Cisco IOS XE Everest 16.6.1 software image to flash, by using the `install add file activate commit` command.

```
Switch# install add file flash:cat9k_iosxe.16.06.01.SPA.bin activate commit
```

```
install_add_activate_commit: START tue Jul 10 19:54:51 UTC 2018
System configuration has been modified.
Press Yes(y) to save the configuration and proceed.
Press No(n) for proceeding without saving the configuration.
Press Quit(q) to exit, you may save configuration and re-enter the command. [y/n/q]y
Building configuration...
[OK] Modified configuration has been saved
* Jul 10 19:54:55.633: %IOSXE-5-PLATFORM: Switch 1 R0/0: Oct 30 19:54:55 install_engine.sh: %INSTALL-5-INSTALL_START_INFO: Started install one-shot flash:cat9k_iosxe.16.06.01.SPA.bin
install_add_activate_commit: Adding PACKAGE
This operation requires a reload of the system. Do you want to proceed?
Please confirm you have changed boot config to flash:packages.conf [y/n]y

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_iosxe.16.06.01.SPA.bin to the selected switch(es)
Finished initial file syncing

--- Starting Add ---
Performing Add on all members
[1] Add package(s) on switch 1
[1] Finished Add on switch 1
Checking status of Add on [1]
Add: Passed on [1]
Finished Add

install_add_activate_commit: Activating PACKAGE
Following packages shall be activated:
  /flash/cat9k-wlc.16.06.01.SPA.pkg
  /flash/cat9k-webui.16.06.01.SPA.pkg
  /flash/cat9k-srdriver.16.06.01.SPA.pkg
  /flash/cat9k-sipspa.16.06.01.SPA.pkg
  /flash/cat9k-sipbase.16.06.01.SPA.pkg
  /flash/cat9k-rpboot.16.06.01.SPA.pkg
  /flash/cat9k-rpbase.16.06.01.SPA.pkg
  /flash/cat9k-guestshell.16.06.01.SPA.pkg
  /flash/cat9k-espbase.16.06.01.SPA.pkg
  /flash/cat9k-cc_srdriver.16.06.01.SPA.pkg

This operation requires a reload of the system. Do you want to proceed? [y/n]y

--- Starting Activate ---
Performing Activate on all members
[1] Activate package(s) on switch 1
[1] Finished Activate on switch 1
Checking status of Activate on [1]
Activate: Passed on [1]
Finished Activate

--- Starting Commit ---
Performing Commit on all members

*Jul 10 19:57:41.145: %IOSXE-5-PLATFORM: Switch 1 R0/0: Jul 10 19:57:41 rollback_timer.sh: %INSTALL-
5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Install auto abort timer will expire in 7200 seconds
[1] Commit package(s) on switch 1
[1] Finished Commit on switch 1
Checking status of Commit on [1]
Commit: Passed on [1]
Finished Commit

Install will reload the system now!
SUCCESS: install_add_activate_commit Tue Jul 10 19:57:48 UTC 2018
Switch#

Note: The system reloads automatically after executing the install add file activate commit command. You do not have to manually reload the system.

Step 4: Reload
a) reload

Use this command to reload the switch.

Switch# reload

b) boot flash:

If your switches are configured with auto boot, then the stack will automatically boot up with the new image. If not, you can manually boot flash:packages.conf

Switch: boot flash:packages.conf

Note: When you downgrade the software image, the boot loader does not automatically downgrade. It remains updated.

c) show version

After the image boots up, use this command to verify the version of the new image.

Note: When you boot the new image, the boot loader is automatically updated, but the new bootloader version is not displayed in the output until the next reload.

The following sample output of the show version command displays the Cisco IOS XE Everest 16.6.1 image on the device:

Switch# show version
Cisco IOS XE Software, Version 16.06.01
Cisco IOS Software [Everest], Catalyst L3 Switch Software (CAT9K_IOSXE), Version 16.6.1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2017 by Cisco Systems, Inc.
Compiled Fri 16-Mar-18 06:38 by mcpre
<output truncated>
Licensing

This section provides information about the licensing packages for features available on Cisco Catalyst 9000 Series Switches.

License Levels

The software features available on Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance fall under these base or add-on license levels.

Base Licenses

- Network Essentials
- Network Advantage—Includes features available with the Network Essentials license and more.

Add-On Licenses

Add-On Licenses require a Network Essentials or Network Advantage as a pre-requisite. The features available with add-on license levels provide Cisco innovations on the switch, as well as on the Cisco Digital Network Architecture Center (Cisco DNA Center).

- DNA Essentials
- DNA Advantage—Includes features available with the DNA Essentials license and more.

To find information about platform support and to know which license levels a feature is available with, use Cisco Feature Navigator. To access Cisco Feature Navigator, go to https://www.cisco.com/go/cfn. An account on cisco.com is not required.

License Types

The following license types are available:

- Permanent—for a license level, and without an expiration date.
- Term—for a license level, and for a three, five, or seven year period.
- Evaluation—a license that is not registered.

License Levels - Usage Guidelines

- Base licenses (Network Essentials and Network-Advantage) are ordered and fulfilled only with a permanent license type.

- Add-on licenses (DNA Essentials and DNA Advantage) are ordered and fulfilled only with a term license type.

- An add-on license level is included when you choose a network license level. If you use DNA features, renew the license before term expiry, to continue using it, or deactivate the add-on license and then reload the switch to continue operating with the base license capabilities.
• When ordering an add-on license with a base license, note the combinations that are permitted and those that are not permitted:

<table>
<thead>
<tr>
<th></th>
<th>DNA Essentials</th>
<th>DNA Advantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Essentials</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Network Advantage</td>
<td>Yes¹</td>
<td>Yes</td>
</tr>
</tbody>
</table>

¹ You will be able to purchase this combination only at the time of the DNA license renewal and not when you purchase DNA-Essentials the first time.

• Evaluation licenses cannot be ordered. They are unregistered licenses that expire after a 90-day period. Warning system messages about the evaluation license expiry are generated 10 and 5 days before the 90-day window. After the 90-day period, warning system messages are generated on a weekly basis. An expired evaluation license cannot be reactivated after reload.

### Smart Licensing

Cisco Smart Licensing is a unified license management system that manages all the software licenses across Cisco products.

It enables you to purchase, deploy, manage, track and renew Cisco Software. It provides information about license ownership and consumption through a single user interface.

The solution is composed of Smart Accounts and Cisco Smart Software Manager. The former is an online account of your Cisco software assets and is required to use the latter. Cisco Smart Software Manager is where you can perform all your licensing management related tasks, such as, registering, de-registering, moving, and transferring licenses. Users can be added and given access and permissions to the smart account and specific virtual accounts.

**Important** Cisco Smart Licensing is the default and the only available method to manage licenses.

### Deploying Smart Licensing

The following provides a process overview of a day 0 to day N deployment directly initiated from a device that is running Cisco IOS XE Fuji 16.9.1 or later releases. Links to the configuration guide provide detailed information to help you complete each one of the smaller tasks.

**Procedure**

**Step 1**
Begin by establishing a connection from your network to Cisco Smart Software Manager on cisco.com.
See: Connecting to CSSM

**Step 2**
Create and activate your Smart Account, or login if you already have one.
To create and activate Smart Account, go to Cisco Software Central → Create Smart Accounts. Only authorized users can activate the Smart Account.
Step 3

Complete Cisco Smart Software Manager set up.

a) Accept the Smart Software Licensing Agreement.

b) Set up the required number of Virtual Accounts, users and access rights for the virtual account users.

   Virtual accounts help you organize licenses by business unit, product type, IT group, and so on.

c) Generate the registration token in the Cisco Smart Software Manager portal and register your device with the token.

   See: Registering the Device in CSSM

With this,

- The device is now in an authorized state and ready to use.
- The licenses that you have purchased are displayed in your Smart Account.

How Upgrading or Downgrading Software Affects Smart Licensing

Starting from Cisco IOS XE Fuji 16.9.1, Smart Licensing is the default and only license management solution; all licenses are managed as Smart Licenses.

Important

Starting from Cisco IOS XE Fuji 16.9.1, the Right-To-Use (RTU) licensing mode is deprecated, and the associated license right-to-use command is no longer available on the CLI.

Note how upgrading to a release that supports Smart Licensing or moving to a release that does not support Smart Licensing affects licenses on a device:

- When you upgrade from an earlier release to one that supports Smart Licensing—all existing licenses remain in evaluation mode until registered in Cisco Smart Software Manager. After registration, they are made available in your Smart Account.

  See: Registering the Device in CSSM

- When you downgrade to a release where Smart Licensing is not supported—all smart licenses on the device are converted to traditional licenses and all smart licensing information on the device is removed.

Using Smart Licensing on an Out-of-the-Box Device

Starting from Cisco IOS XE Fuji 16.9.1, if an out-of-the-box device has the software version factory-provisioned, all licenses on such a device remain in evaluation mode until registered in Cisco Smart Software Manager. See: Registering the Device in CSSM

Scaling Guidelines

For information about feature scaling guidelines, see the Cisco Catalyst 9500 Series Switches datasheet at:
Limitations and Restrictions

With Cisco Catalyst 9500 Series Switches and Cisco Catalyst 9500 Series Switches - High Performance—If a feature is not supported on a switch model, you do not have to factor in any limitations or restrictions that may be listed here. If limitations or restrictions are listed for a feature that is supported, check if model numbers are specified, to know if they apply. If model numbers are not specified, the limitations or restrictions apply to all models in the series.

• Cisco StackWise Virtual—You cannot configure Cisco StackWise Virtual links on the uplink (network) modules (C9500-NM-8X and C9500-NM-2Q).

• Cisco TrustSec restrictions—Cisco TrustSec can be configured only on physical interfaces, not on logical interfaces.

• Flexible NetFlow limitations
  • You cannot configure NetFlow export using the Ethernet Management port (GigabitEthernet0/0).
  • You can not configure a flow monitor on logical interfaces, such as switched virtual interfaces (SVIs), port-channel, loopback, tunnels.
  • You can not configure multiple flow monitors of same type (ipv4, ipv6 or datalink) on the same interface for same direction.

• Hardware limitations:
  • Use the MODE button to switch-off the beacon LED.
  • All port LED behavior is undefined until interfaces are fully initialized.
  • The following limitations apply to Cisco QSA Module (CVR-QSFP-SFP10G) when Cisco 1000Base-T Copper SFP (GLC-T) or Cisco 1G Fiber SFP Module for Multimode Fiber are plugged into the QSA module:
    • 1G Fiber modules over QSA do not support autonegotiation. Auto-negotiation should be disabled on the far-end devices.
    • Although visible in the CLI, the command [no] speed nonegotiate is not supported with 1G Fiber modules over QSA.
    • Only GLC-T over QSA supports auto-negotiation.
    • GLC-T supports only port speed of 1000 Mb/s over QSA. Port speeds of 10/100-Mb/s are not supported due to hardware limitation.
  • When you use Cisco QSFP-4SFP10G-CUXM Direct-Attach Copper Cables, autonegotiation is enabled by default. If the other end of the line does not support autonegotiation, the link does not come up.

• Interoperability limitations:
  • When you use Cisco QSFP-4SFP10G-CUXM Direct-Attach Copper Cables, if one end of the 40G link is a Catalyst 9400 Series Switch and the other end is a Catalyst 9500 Series Switch, the link does not come up, or comes up on one side and stays down on the other. To avoid this interoperability issue between devices, apply the the speed nonegotiate command on the Catalyst 9500 Series Switches.
Switch interface. This command disables autonegotiation and brings the link up. To restore autonegotiation, use the `no speed nonegotiation` command.

- Memory leak—When a logging discriminator is configured and applied to a device, memory leak is seen under heavy syslog or debug output. The rate of the leak is dependent on the quantity of logs produced. In extreme cases, the device may fail. As a workaround, disable the logging discriminator on the device.

- QoS restrictions
  - When configuring QoS queuing policy, the sum of the queuing buffer should not exceed 100%.
  - For QoS policies, only switched virtual interfaces (SVI) are supported for logical interfaces.
  - QoS policies are not supported for port-channel interfaces, tunnel interfaces, and other logical interfaces.

- Secure Shell (SSH)
  - Use SSH Version 2. SSH Version 1 is not supported.
  - When the device is running SCP and SSH cryptographic operations, expect high CPU until the SCP read process is completed. SCP supports file transfers between hosts on a network and uses SSH for the transfer.

  Since SCP and SSH operations are currently not supported on the hardware crypto engine, running encryption and decryption process in software causes high CPU. The SCP and SSH processes can show as much as 40 or 50 percent CPU usage, but they do not cause the device to shutdown.

- VLAN Restriction—It is advisable to have well-defined segregation while defining data and voice domain during switch configuration and to maintain a data VLAN different from voice VLAN across the switch stack. If the same VLAN is configured for data and voice domains on an interface, the resulting high CPU utilization might affect the device.

- Wired Application Visibility and Control limitations:
  - NBAR2 (QoS and Protocol-discovery) configuration is allowed only on wired physical ports. It is not supported on virtual interfaces, for example, VLAN, port channel nor other logical interfaces.
  - NBAR2 based match criteria ‘match protocol’ is allowed only with marking or policing actions. NBAR2 match criteria will not be allowed in a policy that has queuing features configured.
  - ‘Match Protocol’: up to 256 concurrent different protocols in all policies.
  - NBAR2 and Legacy NetFlow cannot be configured together at the same time on the same interface. However, NBAR2 and wired AVC Flexible NetFlow can be configured together on the same interface.
  - Only IPv4 unicast (TCP/UDP) is supported.
  - AVC is not supported on management port (Gig 0/0)
  - NBAR2 attachment should be done only on physical access ports. Uplink can be attached as long as it is a single uplink and is not part of a port channel.
  - Performance—Each switch member is able to handle 500 connections per second (CPS) at less than 50% CPU utilization. Above this rate, AVC service is not guaranteed.
• Scale—Able to handle up to 5000 bi-directional flows per 24 access ports and 10000 bi-directional flows per 48 access ports.

• YANG data modeling limitation—A maximum of 20 simultaneous NETCONF sessions are supported.

Caveats

Caveats describe unexpected behavior in Cisco IOS releases. Caveats listed as open in a prior release are carried forward to the next release as either open or resolved.

Cisco Bug Search Tool

The Cisco Bug Search Tool (BST) allows partners and customers to search for software bugs based on product, release, and keyword, and aggregates key data such as bug details, product, and version. The BST is designed to improve the effectiveness in network risk management and device troubleshooting. The tool has a provision to filter bugs based on credentials to provide external and internal bug views for the search input.

To view the details of a caveat, click on the identifier.

Open Caveats in Cisco IOS XE Fuji 16.9.x

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Applicable Models</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvh85225</td>
<td>All models</td>
<td>Smart licensing(SL)Actions done soon after system bootup can cause SL to get stuck, requiring reload</td>
</tr>
<tr>
<td>CSCvk02773</td>
<td>All models</td>
<td>Standby crashed when defaulting vlan config reconfig vlan config with fnf/et-analytics</td>
</tr>
<tr>
<td>CSCvm79234</td>
<td>All models</td>
<td>Show version cli shows invalid USB-SSD disk size on a CAT9k switch</td>
</tr>
<tr>
<td>CSCvh30574</td>
<td>Catalyst 9500</td>
<td>[SCALE] AVB QoS Crash &quot;Packet Buffer Complex Stalled&quot; with avb/no avb and overnight traffic</td>
</tr>
<tr>
<td>CSCvi48988</td>
<td>Catalyst 9500</td>
<td>SNMP timeout when querying entSensorValueEntry</td>
</tr>
<tr>
<td>CSCvm81361</td>
<td>Catalyst 9500</td>
<td>3850 stack SVL link status incorrect</td>
</tr>
<tr>
<td>CSCve65787</td>
<td>Catalyst 9500 High Performance</td>
<td>Autoneg support for 100G/40G/25G Cu xcvr</td>
</tr>
<tr>
<td>CSCvi44797</td>
<td>Catalyst 9500 High Performance</td>
<td>C9500-48Y4C: TestPhyLoopback showing Untested for some 1G interfaces</td>
</tr>
<tr>
<td>CSCvk39569</td>
<td>Catalyst 9500 High Performance</td>
<td>C9500-48Y4C/C9500-24Y4C : FEC CL91 config is removed after upgrading to 16.9.1 and link goes down</td>
</tr>
<tr>
<td>CSCvk39589</td>
<td>Catalyst 9500 High Performance</td>
<td>Transceiver is removed and inserted syslog when configured 10G mode for SFP-10/25GbE-CSR</td>
</tr>
</tbody>
</table>
## Resolved Caveats in Cisco IOS XE Fuji 16.9.2

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Applicable Models</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvg81784</td>
<td>All models</td>
<td>Converting a layer 2 port-channel to L3 causes some Protocols to break</td>
</tr>
<tr>
<td>CSCvj16271</td>
<td>All models</td>
<td>Addressing memory leaks in IPC error handling cases in LED, RPS, VMARGIN, USB, THERMAL</td>
</tr>
<tr>
<td>CSCvj66609</td>
<td>All models</td>
<td>DHCP offer received from SVI sent back to the same SVI when DHCP Snooping is enabled</td>
</tr>
<tr>
<td>CSCvj75719</td>
<td>All models</td>
<td>System returning incorrect portchannel MIB value (IEEE8023-LAG-MIB)</td>
</tr>
<tr>
<td>CSCvk53444</td>
<td>All models</td>
<td>Packets with Fragment Offset not forwarded with DHCP Snooping Enabled</td>
</tr>
<tr>
<td>CSCvm07921</td>
<td>All models</td>
<td>OOB TX path excessive congestion cause software to force crash a switch</td>
</tr>
<tr>
<td>CSCvj74923</td>
<td>Catalyst 9500</td>
<td>Client does not get the reserved IP Address for the interface on Port based DHCP configuration.</td>
</tr>
<tr>
<td>CSCvk22204</td>
<td>Catalyst 9500</td>
<td>stackwise virtual will blackhole traffic on standby unit after switchover, NIF is stuck</td>
</tr>
<tr>
<td>CSCvk33369</td>
<td>Catalyst 9500</td>
<td>Stack-merge on Stby and CONN_ERR_CONN_TIMEOUT_ERR on Active with multiple SWO</td>
</tr>
<tr>
<td>CSCvk33624</td>
<td>Catalyst 9500</td>
<td>SFF8472-3-READ_ERROR message seen for SVL ports</td>
</tr>
<tr>
<td>CSCvk59766</td>
<td>Catalyst 9500</td>
<td>QSA adapters using 1 gig SFP stop working</td>
</tr>
<tr>
<td>CSCvm36748</td>
<td>Catalyst 9500</td>
<td>FED crash at expired &quot;FED MAC AGING TIMER&quot; or &quot;unknown&quot; timer without a stack trace.</td>
</tr>
<tr>
<td>CSCvk35488</td>
<td>Catalyst 9500 High Performance</td>
<td>C9500-24Y4C:&quot;speed 10000&quot; config is rejected on C9500-24Y4C bootup for SFP-10/25GBase-CSR</td>
</tr>
<tr>
<td>CSCvk52742</td>
<td>Catalyst 9500 High Performance</td>
<td>1G SFP do not link up when connected to C9500-24Y4C/C9500-48Y4C</td>
</tr>
</tbody>
</table>

## Resolved Caveats in Cisco IOS XE Fuji 16.9.1

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Applicable Models</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCvh28104</td>
<td>All models</td>
<td>QSFP-H40G-CU5M 40g not showing as up on peer</td>
</tr>
<tr>
<td>CSCvh63530</td>
<td>All models</td>
<td>MPLS traffic drops with ECMP loadbalance towards core. All cat9ks</td>
</tr>
<tr>
<td>Identifier</td>
<td>Applicable Models</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCvh96261</td>
<td>All models</td>
<td>EXP based Queuing on cat9k platforms</td>
</tr>
<tr>
<td>CSCvj69569</td>
<td>Catalyst 9500</td>
<td>&quot;sh auth sess sw st&quot; broken and session monitoring sessions coming in sh auth sess in legacy mode.</td>
</tr>
<tr>
<td>CSCvg53159</td>
<td>Catalyst 9500</td>
<td>%SNMP-3-RESPONSE_DELAYED: processing GetNext of cafSessionEntry.2 seen on catalyst switch</td>
</tr>
<tr>
<td>CSCvg58417</td>
<td>Catalyst 9500</td>
<td>Unwanted messages seen during removal of USB 3.0 SSD</td>
</tr>
<tr>
<td>CSCvg67012</td>
<td>Catalyst 9500</td>
<td>Deprecate the option of member flash# in upgrade/downgrade CLI for software install</td>
</tr>
<tr>
<td>CSCvg95580</td>
<td>Catalyst 9500</td>
<td>interface speed config went lost after same FRU OIR with &quot;write mem&quot;</td>
</tr>
<tr>
<td>CSCvh49334</td>
<td>Catalyst 9500</td>
<td>Cat9300 stops forwarding multicast - L3M Failed to allocate REP RI</td>
</tr>
<tr>
<td>CSCvh84345</td>
<td>Catalyst 9500</td>
<td>IOS CLI &quot;show platform software fed switch active punt cause summary&quot; may display negative counts</td>
</tr>
<tr>
<td>CSCvh87131</td>
<td>Catalyst 9500</td>
<td>TRACEBACK: OID cefcModuleEntry crashes the box</td>
</tr>
<tr>
<td>CSCvh92130</td>
<td>Catalyst 9500</td>
<td>downloaded policies hit by traffics were all gone after the second SSO</td>
</tr>
<tr>
<td>CSCvi01682</td>
<td>Catalyst 9500</td>
<td>DOM data not available on SFP with QSA adapter when port is shut down</td>
</tr>
<tr>
<td>CSCvi08459</td>
<td>Catalyst 9500</td>
<td>set different words for username and password, but username shown the same as password</td>
</tr>
<tr>
<td>CSCvi26179</td>
<td>Catalyst 9500</td>
<td>Cat9k crash while accessing OBFL</td>
</tr>
<tr>
<td>CSCvi38191</td>
<td>Catalyst 9500</td>
<td>Memory leak in lman process due to &quot;ld_license_ext.dat&quot; build-up.</td>
</tr>
<tr>
<td>CSCvi39202</td>
<td>Catalyst 9500</td>
<td>DHCP fails when DHCP snooping trust is enabled on uplink etherchannel</td>
</tr>
<tr>
<td>CSCvi71507</td>
<td>Catalyst 9500</td>
<td>C9500: Some SVL can go into P/T state with OIR or HA on some switches</td>
</tr>
<tr>
<td>CSCvi75086</td>
<td>Catalyst 9500</td>
<td>Rapid TDL memory leak in SMD process leads to crash of active switch in stack for ipv6 clients</td>
</tr>
<tr>
<td>CSCvi75488</td>
<td>Catalyst 9500</td>
<td>Ping from client fails with enforcement enabled on known mappings</td>
</tr>
<tr>
<td>CSCvj43609</td>
<td>Catalyst 9500</td>
<td>Incorrect MAC_ADDR gets configured in Rommon</td>
</tr>
<tr>
<td>Identifier</td>
<td>Applicable Models</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CSCvh77186</td>
<td>Catalyst 9500 High Performance</td>
<td>C9500-32C: Number of PSU fans to be reported correctly in show env status</td>
</tr>
<tr>
<td>CSCvh79115</td>
<td>Catalyst 9500 High Performance</td>
<td>C9500-32C: Interfaces takes 5mins to come up after reload</td>
</tr>
<tr>
<td>CSCvh09701</td>
<td>Catalyst 9500 High Performance</td>
<td>Power supply state is marked as fail if it is inserted with power cable connected</td>
</tr>
</tbody>
</table>

**Troubleshooting**

For the most up-to-date, detailed troubleshooting information, see the Cisco TAC website at this URL: [https://www.cisco.com/en/US/support/index.html](https://www.cisco.com/en/US/support/index.html)

Go to **Product Support** and select your product from the list or enter the name of your product. Look under Troubleshoot and Alerts, to find information for the problem that you are experiencing.

**Related Documentation**


Cisco Validated Designs documents at this URL: [https://www.cisco.com/go/designzone](https://www.cisco.com/go/designzone)

**Obtaining Documentation and Submitting a Service Request**

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](https://www.cisco.com).
- To get the business impact you’re looking for with the technologies that matter, visit [Cisco Services](https://www.cisco.com).
- To submit a service request, visit [Cisco Support](https://www.cisco.com).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](https://www.cisco.com).
- To obtain general networking, training, and certification titles, visit [Cisco Press](https://www.cisco.com).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](https://www.cisco.com).